

Appl. No. 09/651,979
Amdt. dated November 30, 2004
Reply to Office Action of September 7, 2004

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Please amend claims 1, 5, 7, 8, 10, 11, and 13 as follows:

1. (currently amended): A portable terminal for encrypting information, the portable terminal comprising:

a display for displaying financial transaction options;

an input for receiving financial data for a financial transaction;

means for generating a new key for the financial transaction, wherein the new key is generated using one or more variable properties of the portable terminal, the one or more variable properties include a history of usage of the portable terminal; and

means for encrypting the financial data with the new key.

2. (original): A portable terminal according to claim 1, wherein the new key is generated when the transaction is executed.

3. (previously presented): A portable terminal according to claim 1, wherein the one or more variable properties of the portable terminal include date and time settings.

Appl. No. 09/651,979
Amdt. dated November 30, 2004
Reply to Office Action of September 7, 2004

4. (original): A terminal according to claim 1, further comprising means for generating a unique challenge in addition to the new key so that a unique challenge can be issued for each transaction.

5. (currently amended): A method of encrypting information by a portable terminal, the method comprising the steps of:

inputting financial data for a financial transaction at the portable terminal;
using one or more variable properties of the portable terminal to obtain a sequence of values for the financial transaction, the one or more variable properties include a history of usage of the portable terminal;

generating a new key based on the sequence of values for the financial transaction; and
encrypting information related to the prepared financial transaction with the new key by the portable terminal;.

6. (original): A method according to claim 5, further comprising the step of:
generating a unique challenge value based on the sequence of values.

7. (currently amended): A method according to claim 5, further comprising the steps of:

encrypting the new key and the unique challenge value using a public key issued by a host; and

Appl. No. 09/651,979
Amdt. dated November 30, 2004
Reply to Office Action of September 7, 2004

transmitting the encrypted new key and the unique challenge value to the host.

8. (currently amended): A method of communicating encrypted information between a portable terminal and a self-service terminal, the method comprising the steps of:

using one or more properties of the portable terminal to obtain a sequence of values, the one or more properties include a history of usage of the portable terminal;

generating a new key based on the sequence of values;

generating a challenge value based on the sequence of values;

encrypting the new key and the challenge value using a public key; and

transmitting the encrypted key and challenge value to the self-service terminal.

9. (original): A method according to claim 8, further comprising the steps of:

generating a new challenge value at the self-service terminal;

encrypting the generated challenge value using the new key;

transmitting the encrypted challenge value to the portable terminal; and

awaiting a correct response to the transmitted challenge value being transmitted by the portable terminal before accepting any subsequent transaction at the self-service terminal.

10. (currently amended): A transaction system comprising:

a self-service terminal; and

a portable terminal to execute an encryption program which is operable to use one or

Appl. No. 09/651,979
Amdt. dated November 30, 2004
Reply to Office Action of September 7, 2004

more variable properties of the portable terminal for obtaining a sequence of values, and for generating a new key based on the sequence of values, the one or more variable properties include a history of usage of the portable terminal.

the portable terminal encrypting information for a financial transaction with the new key, and the portable terminal wirelessly transmitting encrypted information to the self service terminal.

11. (currently amended): A method of determining if a self-service terminal is an authentic terminal, the method comprising the steps of:

using one or more properties of a portable terminal to obtain a sequence of values, the one or more properties include a history of usage of the portable terminal;

generating a new key based on the sequence of values;

generating a challenge value based on the sequence of values;

encrypting the new key and challenge value using a public key provided by an institution;

transmitting the encrypted key and challenge to the self-service terminal;

receiving a response from the self-service terminal, decrypting the response using the new key; and

halting any further transmission unless the decrypted response includes a correct reply to the challenge value.

Appl. No. 09/651,979
Amdt. dated November 30, 2004
Reply to Office Action of September 7, 2004

12. (previously presented): The portable terminal of claim 1 wherein the one or more variable properties includes data stored in a dynamic heap of a memory.

13. (currently amended): A portable terminal for encrypting information, the portable terminal comprising:

a user interface having a display, the display displaying transaction options for a financial transaction, the user interface receiving financial transaction data for the financial transaction;

a memory storing an encryption program;

a controller executing the encryption program to generate a key for the financial transaction, wherein the key is generated using one or more variable properties of the portable terminal, the one or more variable properties include a history of usage of the portable terminal, the controller encrypting the financial data with the key; and

a communication port, in response to the user interface executing the financial transaction, the communication port wirelessly transmitting the encrypted information.

14. (previously presented): The portable terminal of claim 13 wherein the portable terminal is a personal digital assistant (PDA) and the encrypted information is transmitted to an automated teller machine(ATM).

15. (previously presented): The portable terminal of claim 13 wherein the key is a symmetric key.

Appl. No. 09/651,979
Amdt. dated November 30, 2004
Reply to Office Action of September 7, 2004

16. (previously presented): The portable terminal of claim 13 wherein the user interface is a keypad and the financial transaction data includes a personal identification number.

17. (previously presented): The portable terminal of claim 16 wherein the personal identification number is biometric based.

18. (previously presented): The portable terminal of claim 13 wherein the one or more properties include usage history stored in the memory.

19. (previously presented): The method of claim 5 further comprising:
receiving a public key issued by a host computer, wherein the encrypting information step further comprises encrypting information using the public key.

20. (previously presented): The method of claim 8 wherein the step of generating a new key based on the sequence of values further comprises:
splitting a hash value into a first half and a second half; and
encrypting the second half with the first half to produce the new key.